ADVANCES IN MATHEMATICS 17, 25–29 (1975)

A Diophantine Equation Which Arises in the Theory of Finite Groups

PETER CRESCENZO

Department of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455

The theory of finite groups leads to diophantine equations in which the variables are restricted to be *prime*. This paper considers the equation (1) below, which arose in connection with the work of Thomas Berger. (Actually Berger was able to bypass the diophantine problem by using group-theoretic arguments instead.) The author thanks Professor Berger for his assistance in writing this paper.

$$p^m - 2q^n = \pm 1; \quad p, q \text{ prime}; \quad m, n > 1. \tag{1}$$

THEOREM. *With the exception of the relation* $(239)^2 - 2(13)^4 = -1$, *every solution of* (1) *has exponents* $m = n = 2$; *i.e., it comes from a unit* $p - q \cdot 2^{1/2}$ *of the quadratic field* $Q(2^{1/2})$ *for which the coefficients* p, q *are prime.*

Remark 1. The equation $p^m - q^n = 1$; p, q prime; $m, n > 1$ is much simpler: the only solution is $3^2 - 2^3 = 1$. (This fact finds frequent application in the theory of finite groups.) Of course *if we dropped the assumption that* p *and* q *be prime*, then we would have "Catalan's Problem." For a discussion of this famous unsolved problem, see Cassels [1].

Remark 2. As is well known, every solution of the equation $x^2 - 2y^2 = \pm 1$ (with no restriction on x, y) can be derived from the fundamental unit $1 + 2^{1/2}$ of the field $Q(2^{1/2})$: One merely sets $x + y \cdot 2^{1/2} = \pm(1 + 2^{1/2})^k$, odd and even values of k corresponding to different choices of the sign in ± 1. Furthermore, after Lemma 3 below, every solution of (1) has m and n even, so it fits into the format of $x^2 - 2y^2 = \pm 1$. The condition that p and q be prime is equivalent to requiring that x and y be *prime powers*, i.e., that $x = p^{m/2}$ and $y = q^{n/2}$.

Remark 3. Although we have proved that (with one exception) $m = n = 2$ in (1), so that the equation becomes $p^2 - 2q^2 = \pm 1$,

we do not know whether or not there are infinitely many prime pairs p, q that satisfy this equation.

Proof. We will show, by completely elementary means, that $m = 2$ and that n is a power of 2. Then applying a deep result of Ljunggren [2], we arrive at our theorem.

LEMMA 1. *Suppose q is an odd prime and m, n, x are positive integers. If $x^m - 2q^n = \pm 1$, then m is a power of 2. Furthermore the sign of the term ± 1 must be $-$, so the equation becomes $x^m - 2q^n = -1$.*

Proof. We may write $m = 2^s r$, where r is odd. Replacing m by r and x by x^{2^s}, we can assume without loss of generality that m is odd. Suppose $m > 1$. Factor

$$2q^n = (x \mp 1)(x^{m-1} \pm \cdots \pm x + 1).$$

Since x must be odd,

$$2q^k = x \mp 1$$

for some $k < n$. Now $x = 2q^k \pm 1$. A number of the form $1 + wq^k$ where $k < n$ and $(w, q) = 1$ has order q^{n-k} modulo q^n, and a number of the form $-1 + wq^k$ has order $2q^{n-k}$. Since $x^m \equiv \pm 1 \pmod{q^n}$, x has an order that divides m or $2m$ (depending on whether we have $+$ or $-$ respectively), so in either case we obtain

$$q^{n-k} \mid m.$$

A little thought shows that $n - k > k$ (since the term $(x \mp 1)$ in the product for $2q^n$ is clearly smaller than the other term, assuming, as we have, that m is odd and $m > 1$). But now the fact that the *exponent* $m \geqslant q^{n-k} \geqslant q^{n/2}$ leads to absurd inequalities when fed back into the relation $x^m = 2q^n \pm 1$, and we have reached a contradiction.

Having proved m even, the fact that the sign of ± 1 must be $-$, follows by considering congruence (mod 4).

Note. Henceforth we need consider only the equation:

$$p^m - 2q^n = -1; \quad p, q \text{ prime}; \quad m, n > 1. \tag{1'}$$

Lemma 1 rules out the $+$ sign in ± 1 except for $q = 2$; but then the equation becomes $p^m - 2^{n+1} = 1$, which is of the type covered by Remark 1 above.

LEMMA 2. *Suppose r, s, n are positive integers and $n > 1$ is odd. Let $e = 1, 3$ represent the congruence class of n* (mod 4). *Set*

$$A_i = \sum_{\substack{k=0 \\ k \equiv i \pmod 4}}^{n} \binom{n}{k} r^{n-k} s^k; \qquad i = 0, 1, 2, 3.$$

Then $r + s$ divides $A_0 + A_e$ and $r - s$ divides $A_0 - A_e$.

Proof. The proof follows readily upon observing (i) that $\binom{n}{4j} = \binom{n}{n-4j}$ (no deeper properties of the binomial coefficients are involved), (ii) that the mapping $4j \to n - 4j$ gives a one-to-one correspondence between terms in the sum for A_0 and terms in the sum for A_e, and (iii) that $(r \pm s)$ divides evenly into $r^h \pm s^h$ whenever h is odd.

LEMMA 3. *Assume p, q are odd primes and $m, n > 1$. If $p^m - 2q^n = -1$, then both m and n are powers of 2.*

Proof. Where previously we needed only the elementary properties of the rational integers, here we will use the Gaussian integers. We already know from Lemma 1 that m is a power of 2. Set $t = p^{m/2}$. Then

$$q^n = [(t + 1)/2]^2 + [(t - 1)/2]^2.$$

Now $(t + 1)/2$ and $(t - 1)/2$ are relatively prime, so q itself must be a sum of squares, $q = a^2 + b^2$. Now we pass to the Gaussian integers; the same unique factorization considerations that give $q = (a + bi)(a - bi)$ also show that

$$(a + bi)^n = \epsilon[((t + 1)/2) \pm ((t - 1)/2)i] \qquad \text{for some unit } \epsilon.$$

Write $n = 2^d N$ where N is odd. Assume $N > 1$. Write $(a + bi)^{2^d} = (r + si)$, so that

$$(r + si)^N = \epsilon[((t + 1)/2) \pm ((t - 1)/2)i], \qquad \text{with } N \text{ odd.}$$

Let $A_i = \sum_k \binom{N}{k} r^{N-k} s^k$, $i = 0, 1, 2, 3$, be defined as in Lemma 2 above. Then

$$(r + si)^N = (A_0 - A_2) + (A_1 - A_3)i.$$

Since N is odd and the unit ϵ has order dividing 4, we may ignore the effect of ϵ; and then by altering the sign of s if need be, we may assume

$$(r + si)^N = ((t + 1)/2) + ((t - 1)/2)i.$$

That is,

$$t = A_0 + A_1 - A_2 - A_3,$$
$$1 = A_0 - A_1 - A_2 + A_3.$$

Now the binomial theorem gives

$$(r+s)^N = A_0 + A_1 + A_2 + A_3,$$
$$(r-s)^N = A_0 - A_1 + A_2 - A_3.$$

Suppose $N \equiv e \pmod 4$, where $e = 1, 3$. Then, by Lemma 2, $r+s$ divides $A_0 + A_e$, so $r+s$ divides $A_2 + A_{2+e}$ also. Similarly $r-s$ divides $A_0 - A_e$ and $A_2 - A_{2+e}$. Thus,

when $e = 1$, $(r+s) \mid t$ and $(r-s) \mid 1$;

when $e = 3$, the situation is reversed.

In either case, $(r \pm s)$ divides t and $(r \mp s) = \pm 1$. But $t = p^{m/2}$ and p is prime (r, s, t etc. are ordinary integers) so we obtain

$$r \pm s = \pm p^h, \qquad h \leqslant m/2,$$
$$r \mp s = \pm 1.$$

Squaring both equations and adding we get $r^2 + s^2 = (p^{2h}+1)/2$, and remembering that $r^2 + s^2 = q^{2^d}$, we see that

$$q^{2^d} = (p^{2h}+1)/2.$$

Also

$$2q^n = p^m + 1 \qquad \text{or} \qquad 2q^{2^dN} = p^m + 1,$$

so

$$p^m + 1 = 2[(p^{2h}+1)/2]^N.$$

Therefore $(p^{2h}+1) \mid (p^m+1)$. Since N is odd and > 1, $m > 2h$.

Write $2h = 2^z M$ for odd M. So $p^{2^z}+1$ divides $p^{2h}+1$ (since M is odd), and we already know that $p^{2h}+1$ divides p^m+1. Furthermore $m = 2^y$ (by Lemma 1) and $y > z$. However $p^{2^z}+1$ trivially divides $p^{2^{z+1}} - 1$ (difference of squares), and $p^{2^{z+1}} - 1$ divides $p^{2^y} - 1$ by similar high school algebra, so $p^{2^z}+1$ is evenly divisible into $p^m - 1$ (since $m = 2^y$). Previously we had $p^{2^z}+1$ dividing p^m+1, so we have reached a contradiction, based on the assumption that $N > 1$.

LEMMA 4. *If p, q are odd primes, m, $n > 1$, and $p^m - 2q^n = -1$, then $m = 2$ and n is a power of 2.*

Proof. From our previous results, both m and n must be powers of 2. Assume $4 \mid m$. Then we have a solution to the equation

$$x^4 - 2y^2 = -1.$$

This can be rewritten

$$y^4 - x^4 = [(x^4 - 1)/2]^2,$$

which is of the type $a^4 - b^4 = c^2$ proved by Fermat to have only the trivial solution $c = 0$, giving $x = y = 1$ (cf. Uspensky [4, p. 403]).

Completion of the proof. After Lemma 4, we have only to consider the possibility that $m = 2$ and $4 \mid n$. This leads to the equation

$$x^2 - 2y^4 = -1.$$

This is much more difficult, but the solution has been found by Ljunggren [2]; see also the book of Mordell [3, p. 271]. The above equation has only the two solutions (1, 1) and (239, 13), which gives us our result.

Remark. Of course Ljunggren's result is very strong inasmuch as it does not require the integers x and y to be prime. Thus it automatically applies to the equation $x^m - 2y^n = -1$ whenever $2 \mid m$ and $4 \mid n$. Our contribution is to eliminate the possibility of odd exponents m, or of n not divisible by 4, and it is here that we use the hypothesis that x and y are prime.

REFERENCES

1. J. W. S. CASSELS, On the equation $a^x - b^y = 1$. II, *Proc. Cambridge Philos. Soc.* **56** (1960), 97–103.
2. W. LJUNGGREN, "Zur Theorie der Gleichung $x^2 + 1 = Dy^4$," Avh. Norske Vid. Akad. Oslo, No. 51, 1942.
3. L. J. MORDELL, "Diophantine Equations," Academic Press, New York, 1969.
4. J. V. USPENSKY AND M. A. HEASLET, "Elementary Number Theory," McGraw-Hill, New York, 1939.